IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
KASSER

Serial No. **Not Yet Assigned**

Filing Date: **Herewith**

For: **METHOD AND SYSTEM FOR SECURE DISTRIBUTION OF DIGITAL DOCUMENTS**

I HEREBY CERTIFY THIS PAPER OR FEE IS BEING DEPOSITED WITH THE U.S. POSTAL SERVICE "EXPRESS MAIL POST OFFICE TO ADDRESSEE" SERVICE UNDER 37 CFR 1.10 ON THE DATE INDICATED BELOW AND IS ADDRESSED TO: MS PATENT APPLICATION, PO BOX 1450, ALEXANDRIA, VA 22313-1450.

EXPRESS MAIL NO: EV330385736US

DATE OF DEPOSIT: March 12, 2004

NAME: Justin Goree

SIGNATURE: Justin Goree

TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT

MS PATENT APPLICATION
COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

Sir:

Transmitted herewith is a certified copy of the French Application No. 0111890.

Respectfully submitted,

Michael W. Taylor

MICHAEL W. TAYLOR
Reg. No. 43,182
Allen, Dyer, Doppelt, Milbrath & Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Post Office Box 3791
Orlando, Florida 32802
Telephone: 407/841-2330
Fax: 407/841-2343
Attorney for Applicant

R E P U B L I Q U E F R A N Ç A I S E

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 04 OCT. 2001

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint Petersbourg
75800 PARIS cedex 08
Téléphone : 33 (1) 53 04 53 04
Télécopie : 33 (1) 42 93 59 30
www.inpi.fr

ETABLISSEMENT PUBLIC NATIONAL CREE PAR LA LOI N° 51-444 DU 19 AVRIL 1951

1er dépôt

INPI
INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE
26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 94 86 54

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11354*01

REQUÊTE EN DÉLIVRANCE 1/2

Remplir impérativement la 2ème page.

Cet imprimé est à remplir lisiblement à l'encre noire DB 540 W / 190600

Réservé à l'INPI

REMISE DES PIÈCES
DATE 14 SEPT 2001
LIEU 13 INPI MARSEILLE
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0111890
DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI 14 SEP. 2001

Vos références pour ce dossier *(facultatif)* 100142 FR

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

OMNIPAT
MARCHAND André
24 Place des Martyrs de la Résistance
13100 AIX EN PROVENCE
FRANCE

Confirmation d'un dépôt par télécopie ☐ N° attribué par l'INPI à la télécopie

2 NATURE DE LA DEMANDE	**Cochez l'une des 4 cases suivantes**	
Demande de brevet	☒	
Demande de certificat d'utilité	☐	
Demande divisionnaire	☐	
Demande de brevet initiale	N°	Date / /
ou demande de certificat d'utilité initiale	N°	Date / /
Transformation d'une demande de brevet européen *Demande de brevet initiale*	☐ N°	Date / /

3 TITRE DE L'INVENTION (200 caractères ou espaces maximum)

Procédé et système de distribution sécurisée de documents numériques

4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE	Pays ou organisation Date / / N°
	Pays ou organisation Date / / N°
	Pays ou organisation Date / / N°
	☐ **S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»**

5 DEMANDEUR		☐ **S'il y a d'autres demandeurs, cochez la case et utilisez l'imprimé «Suite»**
Nom ou dénomination sociale		STMICROELECTRONICS
Prénoms		
Forme juridique		SOCIETE ANONYME
N° SIREN		3 4 1 4 5 9 3 8 6
Code APE-NAF		3 2 1 B
Adresse	Rue	29, Boulevard Romain Rolland
	Code postal et ville	92120 MONTROUGE
Pays		FRANCE
Nationalité		
N° de téléphone *(facultatif)*		
N° de télécopie *(facultatif)*		
Adresse électronique *(facultatif)*		

1er dépôt

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

REQUÊTE EN DÉLIVRANCE 2/2

Cadre réservé à l'INPI

REMISE DES PIÈCES
DATE 14 SEPT 2001
LIEU 13 INPI MARSEILLE
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0111890

DB 540 W /190600

Vos références pour ce dossier : *(facultatif)*		100142 FR
6 MANDATAIRE		
Nom		MARCHAND
Prénom		André
Cabinet ou Société		OMNIPAT
N °de pouvoir permanent et/ou de lien contractuel		
Adresse	Rue	24 Place des Martyrs de la Résistance
	Code postal et ville	13100 AIX EN PROVENCE
N° de téléphone *(facultatif)*		04.42.99.06.60
N° de télécopie *(facultatif)*		04.42.99.06.69
Adresse électronique *(facultatif)*		
7 INVENTEUR (S)		
Les inventeurs sont les demandeurs		☐ Oui ☒ Non **Dans ce cas fournir une désignation d'inventeur(s) séparée**
8 RAPPORT DE RECHERCHE		**Uniquement pour une demande de brevet (y compris division et transformation)**
Établissement immédiat ou établissement différé		☒ ☐
Paiement échelonné de la redevance		**Paiement en deux versements, uniquement pour les personnes physiques** ☐ Oui ☒ Non
9 RÉDUCTION DU TAUX DES REDEVANCES		**Uniquement pour les personnes physiques** ☐ Requise pour la première fois pour cette invention *(joindre un avis de non-imposition)* ☐ Requise antérieurement à ce dépôt *(joindre une copie de la décision d'admission pour cette invention ou indiquer sa référence) :*
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes		

10 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (Nom et qualité du signataire)
MARCHAND André - CPI N° 95 0303
OMNIPAT

VISA DE LA PRÉFECTURE OU DE L'INPI

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire.
Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

PROCEDE ET SYSTEME DE DISTRIBUTION SECURISEE DE DOCUMENTS NUMERIQUES

La présente invention concerne un procédé et un système de distribution sécurisée de documents numériques.

Elle s'applique notamment, mais non exclusivement, à la distribution d'œuvres musicales sous forme numérisée, que ce soit sur des supports d'enregistrement tels que des CDROM, ou par l'intermédiaire d'un réseau public de transmission de données tel que le réseau Internet. Elle vise en particulier à lutter contre la diffusion illégale par le réseau Internet d'œuvres protégées, telles que des œuvres musicales, littéraires ou cinématographiques, ou encore des logiciels.

Depuis l'apparition du réseau Internet et de standards de codage et de compression de données audionumériques tels que "MPEG" ou "mp3", la diffusion de copies illégales d'œuvres musicales s'est développée d'une manière très importante. Plus récemment, se sont constitués des services d'échange de fichiers, accessibles par le réseau Internet. Ces services proposent le téléchargement d'un logiciel permettant à n'importe quel utilisateur du réseau Internet disposant d'un micro-ordinateur, d'accéder à des listes de fichiers qu'il peut télécharger, et en échange, d'offrir un accès libre à certains fichiers mémorisés sur le disque dur de son micro-ordinateur, dont les références et chemins d'accès sont à cet effet insérées dans l'une de ces listes. Il s'avère que ces services ont rencontré un très grand succès parmi les utilisateurs du réseau Internet, lesquels peuvent ainsi à très peu de frais constituer une bibliothèque personnelle d'œuvres musicales ou vidéo, mais aussi de logiciels. Les copies illégales d'œuvres ont donc décuplé à tel point qu'elles sont estimées à plusieurs millions par an.

Pour contrôler la distribution de documents numériques, on a déjà proposé des techniques par lesquelles un client peut consulter un catalogue de documents accessibles par l'intermédiaire d'un réseau public de transmission de données numériques, et sélectionner des documents qu'il souhaite acheter. Un logiciel installé sur le terminal du client envoie sous une forme cryptée les informations d'identification de la carte bancaire du client à un organisme distributeur, et celui-ci transmet au client, également sous une forme cryptée, les documents sélectionnés. Le logiciel installé sur le terminal du client utilise alors une clé secrète pour décrypter les documents reçus, afin de pouvoir les utiliser.

Toutefois, même si le document est protégé par cryptage pendant sa transmission au client, on ne peut pas en empêcher une distribution ultérieure non autorisée, une fois qu'il est décrypté par le client.

Pour résoudre ce problème, on a également proposé une technique par laquelle un mot de passe est vendu au client pour décrypter un document chargé sur une machine de restitution du document, ce mot de passe n'étant utilisable que sur la machine du client ou uniquement par le client en complément d'informations biométriques spécifiques de ce dernier. Même si le document crypté peut être distribué à d'autres personnes, le mot de passe du client sans les informations biométriques ne permet pas décrypter le document.

Il a également été envisagé un système de distribution dans lequel les documents sont distribués sous forme cryptée, et dans lequel les utilisateurs peuvent acheter des licences de reproduction de ces documents, qui sont stockées sur une carte à puce personnelle mise à la disposition de chaque utilisateur. Cette solution est par exemple décrite dans les documents US 5 754 648 et US 6 035 329.

Puisque les documents sont cryptés, ils peuvent

circuler librement notamment sur le réseau Internet. Pour reproduire un tel document, c'est-à-dire par exemple reproduire l'œuvre musicale qu'il contient, l'utilisateur doit posséder un lecteur approprié qui est capable de lire le contenu crypté du document, lire les informations relatives à la licence, stockées sur la carte à puce et utiliser ces informations pour décrypter le contenu du document. Un tel lecteur est par exemple décrit dans les documents WO 98/42098 et US 5 754 648. Il existe à cet effet de nombreuses techniques de cryptage qui sont utilisées pour authentifier le lecteur et la carte à puce et décrypter le document. Pour réaliser un lecteur "pirate", il est donc nécessaire qu'un tel lecteur puisse s'authentifier en tant que lecteur autorisé. Pour cela, il est nécessaire de disposer d'une clé privée correspondant à une clé publique certifiée de lecteur, chaque lecteur autorisé ayant éventuellement une clé privée unique. La principale faille de ce système apparaît lorsqu'une personne parvient à se procurer la clé privée d'un lecteur autorisé pour réaliser un lecteur "pirate". Dans ce cas, il est possible en achetant des licences de décrypter des documents protégés et diffuser les documents ainsi décryptés. Il est également possible de réaliser un logiciel qui peut être diffusé sur le réseau Internet permettant à n'importe qui possédant un ordinateur et un lecteur de carte à puce d'extraire les licences stockées sur une carte à puce décrypter les documents cryptés correspondants qui sont diffusés librement, et de diffuser d'une manière libre les documents ainsi décryptés.

Il existe par ailleurs un certain nombre de techniques pour insérer des informations dans des puces de manière à ce qu'elles soient très difficilement accessibles. Toutefois, ces techniques ne sont pas totalement sûres et ne peuvent pas prendre en compte des technologies futures que pourraient utiliser les pirates. En outre, ces techniques sont difficilement applicables

aux lecteurs qui sont des systèmes notablement plus complexes que les cartes à puce dans la mesure où ils comprennent un processeur avec davantage d'entrées et sorties, et qui ne sont pas dédiés à la sécurité contrairement aux puces des cartes à puce.

Enfin, contrairement aux applications des cartes à puces, notamment au domaine bancaire et à la téléphonie mobile, la technique décrite précédemment de diffusion sécurisée de documents utilise les cartes à puce dans des lecteurs entièrement déconnectés d'un éventuel système central, si bien que les fraudes ne peuvent pas être aussi facilement détectées que dans les applications utilisant un système central qui peut désactiver une carte à puce préalablement détectée frauduleuse.

Même si cela représente des mois de travail de récupérer la clé privée d'un tel lecteur de documents, cette opération peut être effectuée dans un cadre purement privé et une fois que la clé privée d'un lecteur est obtenue, la sécurité offerte par le système ne peut plus être assurée.

La présente invention a pour but de résoudre ce problème. Cet objectif est atteint par la prévision d'un procédé de diffusion sécurisée de documents numériques en vue de leur restitution sur un lecteur adapté, ces documents étant accessibles sous une forme cryptée, ce procédé comprenant des étapes consistant à :

- attribuer à chaque utilisateur souhaitant restituer un document numérique un moyen de stockage sécurisé d'informations d'identification contenant des informations d'identification du moyen de stockage,
- identifier depuis un serveur connecté à un réseau de transmission de données numériques un moyen de stockage d'informations d'identification, relié au réseau,
- transmettre au serveur des informations d'identification d'un document à restituer, à partir d'un terminal relié au moyen de stockage,

- transmettre en réponse du serveur au terminal une clé de décryptage spécifique du document à restituer qui est mémorisée dans le moyen de stockage,
- décrypter le document à restituer, au moyen d'un lecteur adapté relié au moyen de stockage, à l'aide de la clé de décryptage mémorisée, pour restituer le document décrypté au moyen du lecteur,

caractérisé en ce qu'il comprend en outre des étapes consistant à insérer dans le moyen de stockage des informations d'identification de lecteurs de documents, et déterminer un usage frauduleux du moyen de stockage, en fonction des informations d'identification de lecteurs de documents, mémorisées dans le moyen de stockage.

Avantageusement, le procédé selon l'invention comprend en outre une étape consistant à déterminer par des moyens de traitement associés au moyen de stockage si le lecteur utilisé pour restituer un document est autorisé ou non, la transmission de la clé de décryptage du moyen de stockage au lecteur étant effectuée uniquement si le lecteur est autorisé.

De préférence, si un usage frauduleux du moyen de stockage est déterminé, la transmission du serveur au moyen de stockage de la clé décryptage spécifique du document à restituer n'est pas autorisée, le moyen de stockage est considéré comme ayant été utilisé avec un lecteur non autorisé et désactivé par le serveur pour interdire toute nouvelle utilisation du moyen de stockage pour restituer un document à l'aide d'un lecteur.

Selon une première variante préférée de l'invention, les informations d'identification de lecteurs de documents, mémorisées dans le moyen de stockage, comprennent une liste d'informations d'identification de lecteurs de documents identifiant des lecteurs non autorisés, cette liste étant transmise du serveur au moyen de stockage lors d'une connexion du moyen de stockage au serveur, un usage frauduleux du moyen de stockage étant déterminé si les informations

d'identification du lecteur se trouvent dans la liste des lecteurs non autorisés.

Selon une seconde variante préférée de l'invention, les informations d'identification de lecteurs de documents mémorisées dans le moyen de stockage comprennent une liste d'informations d'identification de lecteurs de documents identifiant les derniers lecteurs de documents utilisés à l'aide du moyen de stockage, cette liste étant transmise du moyen de stockage au serveur lors d'une connexion du moyen de stockage au serveur, en association avec des informations d'identification du moyen de stockage, le serveur comparant les informations d'identification de lecteurs contenues dans la liste reçue avec les informations d'identification de lecteurs contenues dans une liste de lecteurs non autorisés pour déterminer un usage frauduleux du moyen de stockage.

Avantageusement, le serveur constitue à partir des listes reçues d'informations d'identification de lecteurs utilisés, associées à des informations d'identification de moyens de stockage, une table contenant pour chaque lecteur identifié un nombre de moyens de stockage différents utilisé en association avec ce lecteur, et détermine qu'un lecteur est non autorisé si ce nombre pour le lecteur dépasse un seuil prédéfini, et insère dans une liste de lecteurs non autorisés les informations d'identification du lecteur déterminé non autorisé.

Selon une particularité de l'invention, si un usage frauduleux du moyen de stockage est déterminé, la clé demandée de décryptage de document n'est pas transmise du serveur au moyen de stockage.

Selon une autre particularité de l'invention, si un usage frauduleux du moyen de stockage est déterminé, le serveur désactive le moyen de stockage de manière à interdire toute nouvelle utilisation du moyen de stockage pour restituer un document à l'aide d'un lecteur.

La présente invention concerne également un système de diffusion sécurisée de documents numériques en vue de leur restitution sur un lecteur adapté, ces documents étant accessibles sous une forme cryptée, ce système comprenant :

- un moyen de stockage mis à la disposition de chaque utilisateur du système, comportant une zone mémoire sécurisée dans laquelle sont mémorisées des informations d'identification du moyen de stockage,
- un serveur connecté à un réseau de transmission de données numériques,
- au moins un terminal connecté au réseau et muni de moyens de connexion du moyen de stockage, comprenant des moyens de transmission pour transmettre au serveur les informations d'identification du moyen de stockage auquel il est connecté avec des informations d'identification d'un document à restituer, des moyens pour recevoir du serveur une clé de décryptage spécifique permettant de décrypter le document et pour insérer cette clé dans le moyen de stockage auquel il est connecté,
- un lecteur de documents comprenant des moyens de connexion avec l'un des moyens de stockage, des moyens pour recevoir dudit moyen de stockage une clé de décryptage du document à restituer, des moyens pour mémoriser le document à restituer sous forme cryptée, des moyens de décryptage de document à l'aide de la clé de décryptage reçue du moyen de stockage, et des moyens pour restituer le document décrypté,

caractérisé en ce que chaque moyen de stockage comprend en outre une zone mémoire dans laquelle sont mémorisées des informations d'identification d'une liste de lecteurs, et le système comprend des moyens pour déterminer un usage frauduleux du moyen de stockage en fonction du contenu de ladite liste.

Selon la première variante préférée de l'invention, la liste mémorisée dans chaque moyen de stockage comprend

les informations d'identification de lecteurs non autorisés, le serveur comprenant des moyens de transmission pour transmettre cette liste au moyen de stockage par l'intermédiaire du terminal.

Selon la seconde variante préférée de l'invention, la liste mémorisée dans chaque moyen de stockage comprend les informations d'identification des derniers lecteurs utilisés avec le moyen de stockage, le terminal comprenant des moyens pour transmettre cette liste du moyen de stockage au serveur.

De préférence, chaque moyen de stockage est constitué par une carte à microcircuit.

Ces objets, caractéristiques et avantages ainsi que d'autres de la présente invention seront exposés plus en détail dans la description suivante d'un mode de réalisation de l'invention, faite à titre non limitatif en relation avec les figures jointes parmi lesquelles :

- la figure 1 représente schématiquement un système de distribution sécurisé selon l'invention ;
- la figure 2 représente schématiquement un lecteur utilisé dans le système représenté sur la figure 1.

Sur la figure 1, le système selon l'invention comprend un serveur de licences 2 de documents numériques ayant par exemple accès à une bibliothèque 3 de documents numériques à distribuer. Ces documents numériques peuvent contenir des œuvres musicales, audiovisuelles ou littéraires.

Le serveur de licences est relié à cet effet à un ou plusieurs réseaux publics 1 de transmission d'informations numériques tels que le réseau Internet, des réseaux câblés ou de téléphonie mobile ou terrestre, ou encore des systèmes de diffusion radioélectrique terrestre ou par satellite. Les documents à distribuer peuvent également être enregistrés sur des supports 7

tels que des CDROM ou DVD, ou encore des cartes à mémoire de relativement grande capacité telles que des mémoires Flash.

Les utilisateurs souhaitant avoir accès à de tels documents doivent disposer :

- d'une carte à puce 6 personnelle, également appelée carte à microcircuit ou microprocesseur comportant une ou plusieurs mémoires, dont au moins une partie est sécurisée, c'est-à-dire rendue inaccessible, pour pouvoir stocker des informations confidentielles, et
- d'un lecteur 4 adapté à la reproduction de ces documents, et équipé d'un lecteur 16 de carte à puce.

Bien entendu, on peut envisager de combiner dans un même dispositif, la carte à puce et la carte à mémoire permettant de stocker un ou plusieurs documents cryptés.

Les documents enregistrés dans la bibliothèque de documents 3 ou sur les supports 7 sont cryptés, à l'aide d'un algorithme de cryptage symétrique utilisant une clé secrète. Ces documents sont diffusés d'une manière libre, soit par le serveur de licences 2, soit par d'autres organismes.

Pour reproduire de tels documents, un lecteur 4 comme celui représenté sur la figure 2 comprend un processeur 11, par exemple de type microprocesseur ou microcontrôleur, qui est connecté par un bus 14 à des mémoires 12 de données et de programme, ainsi qu'à des moyens de décodage 13 tels qu'un convertisseur numérique analogique pour envoyer le contenu du document une fois décrypté, à des moyens de restitution adéquats, tels qu'un écran vidéo et/ou des haut-parleurs, s'il s'agit par exemple d'un document audiovisuel ou sonore.

Pour recevoir des documents à reproduire, le lecteur 4 comprend avantageusement des moyens de communication 15, constitués par exemple par un modem, et conçus pour se connecter à un réseau 1, et/ou des moyens de lecture 17 de supports d'enregistrement 7 tels que des CDROM et/ou DVD. Si le support d'enregistrement est constitué

par une carte mémoire, le lecteur 4 comprend également ou alternativement, des moyens de connexion pour raccorder au bus 14 la carte mémoire qui est par exemple enfichable dans le boîtier du lecteur 4.

Les mémoires 12 du lecteur 4 mémorisent une paire de clés privée et publique, et éventuellement un code d'identification du lecteur, et comprennent une zone mémoire 21 sécurisée, c'est-à-dire protégée par des moyens connus de manière à être très difficilement accessible, et dans laquelle est stockée notamment la clé privée de décodage utilisée pour décoder la clé secrète de décryptage des documents à reproduire qui est préalablement cryptée par un procédé asymétrique.

Le lecteur 4 comprend en outre un lecteur 16 de carte à puce 6 dans laquelle sont mémorisés une clé publique et d'une manière sécurisée la clé privée 18 correspondante, et éventuellement un code d'identification qui peut être identique à la clé publique de la carte. La carte à puce mémorise également une liste 19 de clés secrètes de décryptage de documents qui ont préalablement été cryptées à l'aide de la clé publique de la carte à puce, chacune de ces clés secrètes étant associée à un identifiant de document dont l'utilisateur de la carte a acheté des licences de reproduction ou de restitution.

Pour remplir cette liste 19 de clés secrètes, l'utilisateur doit accéder au serveur de licences 2, à l'aide d'un terminal 9 (par exemple un ordinateur) connecté au réseau Internet 1 et à un lecteur de carte à puce 10, dans lequel il insère sa carte, et acheter des licences de reproduction de documents. Durant un tel achat, la carte à puce via le terminal 9 transmet sa clé publique et le serveur de licences 2 transmet en retour les clés secrètes de décryptage des documents correspondants préalablement cryptées à l'aide de la clé publique transmise par la carte, les clés secrètes cryptées sont chargées par l'ordinateur et le lecteur de

carte à puce, dans la carte à puce insérée dans ce dernier. Les clés secrètes cryptées transmises peuvent être accompagnées des documents cryptés correspondants.

Lorsque l'utilisateur souhaite reproduire un document déterminé à l'aide de son lecteur 4, il insère dans ce dernier sa carte à puce 6, ainsi que le support d'enregistrement 7 contenant le document crypté à restituer. Ce document peut également avoir été préalablement téléchargé dans la mémoire 12 par l'intermédiaire des moyens de transmission mentionnés ci-avant, ou encore être contenu dans une mémoire externe enfichable dans le lecteur 4.

Le processeur 11 lit le code d'identification du document à restituer et l'envoie à la carte à puce 6, laquelle recherche dans la liste des clés secrètes 19 si l'une de ces clés est associée au code d'identification de document lu et transmis. Si tel est le cas, la carte à puce 6 demande au lecteur sa clé publique, décrypte la clé secrète du document à restituer à l'aide de sa clé privée et crypte cette clé secrète à l'aide de la clé publique fournie par le lecteur. Ensuite, elle transmet la clé secrète cryptée au processeur 11, lequel décrypte la clé secrète puis décrypte le document à l'aide de la clé secrète reçue et décryptée et envoie les informations décryptées contenues dans le document aux moyens de décodage 13 pour restituer ce dernier sur le moyen de restitution adéquat.

La carte à puce exécute une procédure d'authentification de la clé publique reçue du lecteur qui a été préalablement certifiée par une autorité de certification. Cette procédure d'identification consiste généralement à vérifier que la signature qui a été préalablement associée à la clé publique du lecteur correspond à celle de l'autorité de certification, cette signature étant déterminée à l'aide d'une clé publique de l'autorité de certification qui est mémorisée par la carte à puce.

Selon l'invention, lors de l'achat d'une ou plusieurs licences, le serveur de licences 2 transmet à l'utilisateur également une liste de révocation contenant les codes d'identification ou clés publiques certifiées de lecteurs de documents non autorisés, car considérés comme des lecteurs pirates, ou plus généralement des informations permettant d'identifier de tels lecteurs, ces informations étant stockées dans une base de données de lecteurs 8 reliée au serveur de licences 2. Cette liste est mémorisée dès sa réception dans une zone mémoire 20 de la carte à puce.

Ensuite, lorsque la carte à puce 6 est insérée dans un lecteur 4 de documents, le processeur 11 exécute un processus d'identification du lecteur, au cours duquel le lecteur 4 transmet son code d'identification à la puce de la carte 6, et celle-ci vérifie si ce code d'identification se trouve ou non dans la liste 20 des codes d'identification de lecteurs non autorisés. Si le lecteur 4 n'est pas référencé dans cette liste, la carte à puce autorise le décryptage du document en demandant au lecteur de documents le code d'identification du document à restituer et en transmettant en réponse la clé de décryptage correspondant à ce document. Dans le cas contraire, la carte à puce 6 mémorise en mettant à jour la valeur d'un indicateur, qu'elle a été mise en communication avec un lecteur non autorisé, ce qui permet par la suite d'interdire toute nouvelle restitution de document à l'aide de cette carte à puce. Toutefois, le décryptage du document à restituer peut tout de même être autorisé pour ne pas éveiller l'attention de l'utilisateur, et lorsque l'utilisateur se connecte à nouveau au serveur de licences 2 pour acheter de nouvelles licences, et ainsi recevoir les clés de décryptage correspondantes, la valeur de l'indicateur est transmise au serveur de licences 2 avec le code d'identification de la carte à puce. Le serveur de licences 2 peut alors identifier les cartes à puce qui

sont frauduleusement utilisées, et éventuellement refuser de vendre de nouvelles licences aux utilisateurs de telles cartes à puce, ou encore désactiver ces dernières.

Toutefois, cette solution est limitée par la capacité de la mémoire de la carte à puce. En effet, la liste 20 des codes d'identification des lecteurs non autorisés peut devenir trop longue pour pouvoir être stockée par la carte à puce. En outre, cette solution ne permet pas de détecter simplement les lecteurs frauduleux.

Pour résoudre ce problème, la liste 20 des codes de lecteurs non autorisés stockée dans la carte à puce est avantageusement limitée aux plus récents lecteurs détectés frauduleux.

De préférence, la carte à puce 6 stocke également dans sa mémoire à chaque restitution d'un document, le code d'identification du lecteur 4 de documents utilisé.

Avantageusement, la carte à puce 6 gère une liste de codes d'identification des derniers lecteurs utilisés de la manière suivante. A chaque fois que la carte à puce 6 est utilisée dans un lecteur 4, le code d'identification du lecteur transmis à la carte est comparé avec les codes d'identification des derniers lecteurs utilisés, stockés dans une zone mémoire de taille prédéfinie de la carte à puce, et s'il n'y figure pas, il est inséré dans cette zone mémoire qui est avantageusement gérée en FIFO (First-In First-Out), c'est-à-dire qu'un code d'identification est inséré dans cette zone mémoire en remplacement du code mémorisé en premier, si celle-ci est pleine.

A chaque fois que la carte à puce 6 est utilisée pour acheter de nouvelles licences de reproduction de documents, le contenu de cette zone mémoire est transmis avec le code d'identification de la carte à puce au serveur de licences 2, lequel peut ainsi mémoriser dans la base de données 8 les codes d'identification des lecteurs utilisés, et comptabiliser pour chaque code

d'identification de lecteur le nombre de cartes à puce différentes ayant été insérées dans un lecteur identifié par ce code.

Si ce nombre dépasse un certain seuil prédéfini, par exemple 100, pour un code d'identification de lecteur, ce code est alors repéré comme étant celui d'un lecteur frauduleux et inséré dans une liste de révocation de lecteurs non autorisés, gérée par le serveur de licences 2. Lors de l'achat de licences à l'aide d'une carte à puce, le serveur de licences 2 vérifie si un lecteur non autorisé est référencé dans la liste des codes des derniers lecteurs utilisés, mémorisée dans la carte à puce et transmise au serveur. Si tel est le cas, il peut comme précédemment refuser d'accorder les licences demandées, et/ou insérer dans la mémoire de la carte à puce 6 un indicateur pour interdire toute nouvelle utilisation de la carte pour décrypter un document, ou bien commander la désactivation de la carte, ou encore indiquer à la carte à puce les codes d'identification des lecteurs non autorisés figurant dans la liste transmise, de manière à empêcher par la suite que la carte à puce soit utilisée sur un lecteur non autorisé, figurant dans la zone mémoire des derniers lecteurs utilisés.

Il est à noter que si le nombre de codes d'identification mémorisés dans la liste des derniers lecteurs utilisés est suffisant, il n'est plus nécessaire qu'une liste 20 de lecteurs révoqués soit téléchargée par le serveur 2 aux cartes à puce 6.

REVENDICATIONS

1. Procédé de diffusion sécurisée de documents numériques en vue de leur restitution sur un lecteur (4) adapté, ces documents étant accessibles sous une forme cryptée, ce procédé comprenant des étapes consistant à :

- attribuer à chaque utilisateur souhaitant restituer un document numérique un moyen de stockage sécurisé (6) d'informations d'identification contenant des informations d'identification du moyen de stockage,
- identifier depuis un serveur (2) connecté à un réseau de transmission de données numériques (1) un moyen de stockage d'informations d'identification (6), relié au réseau,
- transmettre au serveur (2) des informations d'identification d'un document à restituer, à partir d'un terminal (9) relié au moyen de stockage (6),
- transmettre en réponse du serveur au terminal une clé de décryptage spécifique du document à restituer qui est mémorisée dans le moyen de stockage,
- décrypter le document à restituer, au moyen d'un lecteur (4) adapté relié au moyen de stockage (6), à l'aide de la clé de décryptage mémorisée, pour restituer le document décrypté au moyen du lecteur,

caractérisé en ce qu'il comprend en outre des étapes consistant à insérer dans le moyen de stockage (6) des informations d'identification de lecteurs (4) de documents, et déterminer un usage frauduleux du moyen de stockage, en fonction des informations d'identification de lecteurs de documents, mémorisées dans le moyen de stockage.

2. Procédé selon la revendication 1, caractérisé en ce qu'il comprend en outre une étape consistant à déterminer par des moyens de traitement associés au moyen de stockage (6) si le lecteur (4) utilisé pour restituer un document est autorisé ou non, la transmission de la

clé de décryptage du moyen de stockage au lecteur étant effectuée uniquement si le lecteur est autorisé.

3. Procédé selon la revendication 1 ou 2, caractérisé en ce que si un usage frauduleux du moyen de stockage est déterminé, la transmission du serveur (2) au moyen de stockage (6) de la clé décryptage spécifique du document à restituer n'est pas autorisée, le moyen de stockage est considéré comme ayant été utilisé avec un lecteur (4) non autorisé et désactivé par le serveur pour interdire toute nouvelle utilisation du moyen de stockage pour restituer un document à l'aide d'un lecteur (4) de document.

4. Procédé selon l'une quelconque des revendications 1 à 3, caractérisé en ce que les informations d'identification de lecteurs (4) de documents, mémorisées dans le moyen de stockage (6), comprennent une liste (20) d'informations d'identification de lecteurs de documents identifiant des lecteurs non autorisés, cette liste étant transmise du serveur (2) au moyen de stockage (6) lors d'une connexion du moyen de stockage au serveur, un usage frauduleux du moyen de stockage étant déterminé si les informations d'identification du lecteur se trouvent dans la liste des lecteurs non autorisés.

5. Procédé selon l'une quelconque des revendications 1 à 4, caractérisé en ce que les informations d'identification de lecteurs (4) de documents mémorisées dans le moyen de stockage comprennent une liste (20) d'informations d'identification de lecteurs (4) de documents identifiant les derniers lecteurs de documents utilisés à l'aide du moyen de stockage (6), cette liste étant transmise du moyen de stockage (6) au serveur (2) lors d'une connexion du moyen de stockage au serveur, en association avec des informations d'identification du moyen de stockage, le serveur comparant les informations

d'identification de lecteurs contenues dans la liste reçue avec les informations d'identification de lecteurs contenues dans une liste (8) de lecteurs non autorisés pour déterminer un usage frauduleux du moyen de stockage.

6. Procédé selon la revendication 5, caractérisé en ce que le serveur constitue à partir des listes reçues d'informations d'identification de lecteurs (4) utilisés, associées à des informations d'identification de moyens de stockage (6), une table (8) contenant pour chaque lecteur identifié un nombre de moyens de stockage différents utilisé en association avec ce lecteur, et détermine qu'un lecteur est non autorisé si ce nombre pour le lecteur dépasse un seuil prédéfini, et insère dans une liste de lecteurs non autorisés les informations d'identification du lecteur déterminé non autorisé.

7. Procédé selon l'une quelconque des revendications 1 à 6, caractérisé en ce que si un usage frauduleux du moyen de stockage (6) est déterminé, la clé demandée de décryptage de document n'est pas transmise du serveur (2) au moyen de stockage (6).

8. Procédé selon l'une quelconque des revendications 1 à 7, caractérisé en ce que si un usage frauduleux du moyen de stockage (6) est déterminé, le serveur (2) désactive le moyen de stockage de manière à interdire toute nouvelle utilisation du moyen de stockage pour restituer un document à l'aide d'un lecteur (4).

9. Système de diffusion sécurisée de documents numériques en vue de leur restitution sur un lecteur (4)adapté, ces documents étant accessibles sous une forme cryptée, ce système comprenant :

- un moyen de stockage (6) mis à la disposition de chaque utilisateur du système, comportant une zone mémoire sécurisée (18) dans laquelle sont mémorisées des

informations d'identification du moyen de stockage,
- un serveur (2) connecté à un réseau (1) de transmission de données numériques,
- au moins un terminal (9) connecté au réseau et muni de moyens de connexion du moyen de stockage (6), comprenant des moyens de transmission pour transmettre au serveur (2) les informations d'identification du moyen de stockage auquel il est connecté avec des informations d'identification d'un document à restituer, des moyens pour recevoir du serveur une clé de décryptage spécifique permettant de décrypter le document et pour insérer cette clé dans le moyen de stockage auquel il est connecté,
- un lecteur (4) de documents comprenant des moyens de connexion (16) avec l'un des moyens de stockage (6), des moyens pour recevoir dudit moyen de stockage une clé de décryptage du document à restituer, des moyens pour mémoriser le document à restituer sous forme cryptée, des moyens de décryptage de document à l'aide de la clé de décryptage reçue du moyen de stockage, et des moyens pour restituer le document décrypté,

caractérisé en ce que chaque moyen de stockage (6) comprend en outre une zone mémoire (20) dans laquelle sont mémorisées des informations d'identification d'une liste de lecteurs, et le système comprend des moyens pour déterminer un usage frauduleux du moyen de stockage en fonction du contenu de ladite liste.

10. Système selon la revendication 9, caractérisé en ce que la liste mémorisée dans chaque moyen de stockage (6) comprend les informations d'identification de lecteurs non autorisés, le serveur (2) comprenant des moyens de transmission pour transmettre cette liste au moyen de stockage par l'intermédiaire du terminal (9).

11. Système selon la revendication 9 ou 10, caractérisé en ce que la liste (20) mémorisée dans chaque

moyen de stockage comprend les informations d'identification des derniers lecteurs (4) utilisés avec le moyen de stockage, le terminal (9) comprenant des moyens pour transmettre cette liste du moyen de stockage (6) au serveur (2).

12. Procédé selon l'une quelconque des revendications 9 à 11, caractérisé en ce que chaque moyen de stockage (6) est constitué par une carte à microcircuit.

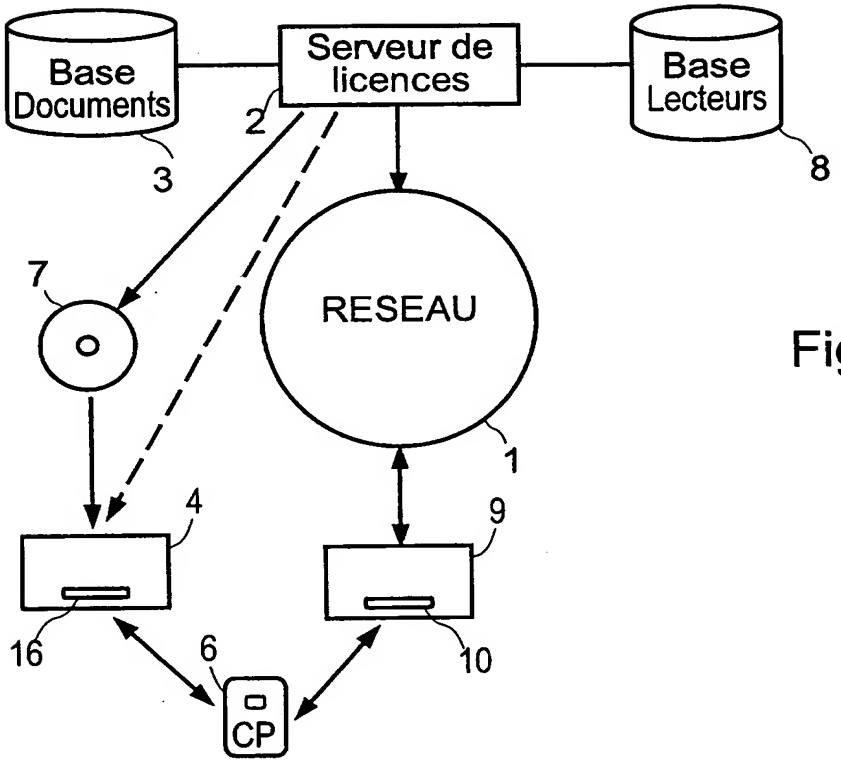
Base Documents
Serveur de licences
Base Lecteurs
RESEAU
CP
1
2
3
4
6
7
8
9
10
16

Fig. 1

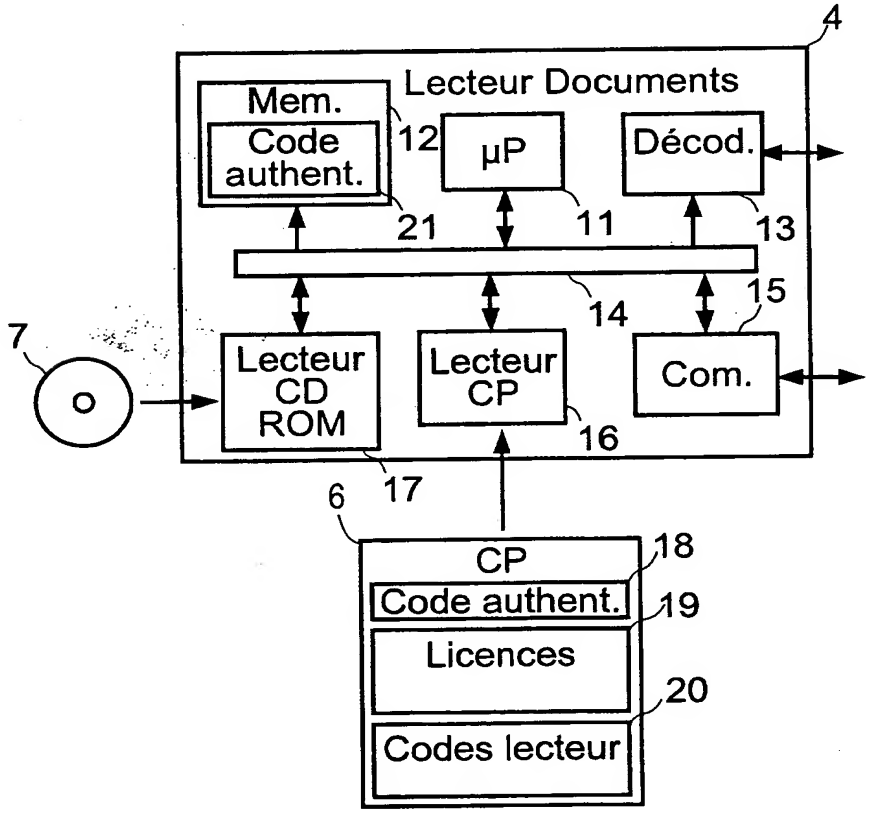
Lecteur Documents
Mem.
Code authent.
µP
Décod.
Com.
Lecteur CD ROM
Lecteur CP
CP
Code authent.
Licences
Codes lecteur
4
6
7
11
12
13
14
15
16
17
18
19
20
21

Fig. 2

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11235*02

DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

DÉSIGNATION D'INVENTEUR(S) Page N° 1../1..
(Si le demandeur n'est pas l'inventeur ou l'unique inventeur)

Cet imprimé est à remplir lisiblement à l'encre noire DB 113 W /260899

Vos références pour ce dossier *(facultatif)*	100142 FR
N° D'ENREGISTREMENT NATIONAL	01 M 890

TITRE DE L'INVENTION (200 caractères ou espaces maximum)

Procédé et système de distribution sécurisée de documents numériques

LE(S) DEMANDEUR(S) :
MARCHAND André
OMNIPAT
24, Place des Martyrs de la Résistance
13100 AIX EN PROVENCE

DESIGNE(NT) EN TANT QU'INVENTEUR(S) : (Indiquez en haut à droite «Page N° 1/1» S'il y a plus de trois inventeurs, utilisez un formulaire identique et numérotez chaque page en indiquant le nombre total de pages).

Nom		KASSER	
Prénoms		Bernard	
Adresse	Rue	C/O OMNIPAT 24 Place des Martyrs de la Résistance	
	Code postal et ville	13100	AIX EN PROVENCE
Société d'appartenance *(facultatif)*			
Nom			
Prénoms			
Adresse	Rue		
	Code postal et ville		
Société d'appartenance *(facultatif)*			
Nom			
Prénoms			
Adresse	Rue		
	Code postal et ville		
Société d'appartenance *(facultatif)*			

DATE ET SIGNATURE(S)
DU (DES) DEMANDEUR(S)
OU DU MANDATAIRE
(Nom et qualité du signataire)
Aix en Provence, le 13 septembre 2001
MARCHAND André - CPI N° 95 0303
OMNIPAT

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.